Minnesota Journal of Law, Science & Technology

Volume 19 | Issue 2 Article 1

6-2018

Rise of the Intelligent Information Brokers: Role of Computational Law Applications in Administering the Dynamic Cybersecurity Threat Surface in IOT

Eran Kahana

Rise of the Intelligent Information Brokers: Role of Computational Law Applications in Administering the Dynamic Cybersecurity Threat Surface in IOT

Eran Kahana*

I. INTRODUCTION

Enter the Internet of Things (IoT). It is widely accepted as the next major milestone in the Internet's evolution. How big of a deal is the IoT? Well, the numbers tell the story: we're looking

* Eran Kahana is a cybersecurity and intellectual property lawyer as well as a Fellow at Stanford Law School. Eran also serves in a variety of cybersecurity thought-leadership roles and works closely with the FBI, Department of Justice, Secret Service, and colleagues from the private and academic sectors to set, promote, and sustain cybersecurity best practices. Eran serves as both general counsel and as a director on the Executive Board of InfraGard (MN Chapter). At Stanford, Eran writes and lectures on the intersect between law and artificial intelligence and is a frequent speaker at Stanford's annual E-Commerce Best Practices Conference. He has been interviewed on cybersecurity, privacy, and technology law at Bloomberg Law, BBC, KABC radio, Minnesota Public Radio, Twin Cities Business magazine, Star Tribune, TheStreet.com, Quartz, and Stanford University Radio, KZSU FM. This paper is built on more than nine years of research at Stanford Law School.

at an ecosystem composed of billions[1] of "things," devices that by 2025 will command trillion-dollar market values.[2] IoT devices differ in size and function but have two things in common: they collect data and have an Internet connection. They can take pretty much any form. Some are kitchen appliances (refrigerators), health activity monitors (FitBit), thermostats (NEST), medical devices (insulin pumps), automated components in automobiles (Tesla over-the-air software updates), drones, and many other implements. Coupled with increasingly sophisticated artificial intelligence capabilities,[3] the IoT ecosystem is poised to generate what could amount to zettabytes[4] of content-rich, valuable data that nefarious actors find irresistible. In this setting, data security—specifically, the tasks of ensuring confidentiality, integrity, and availability[5] of

---

1. *See* Press Release, Gartner, Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent from 2016 (Feb. 7, 2017), https://www.gartner.com/newsroom/id/3598917.

2. *See* James Manyika et al., *Unlocking the Potential of the Internet of Things*, MCKINSEY & CO. (June 2015), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

3. *See* Robert L. Adams, *10 Powerful Examples of Artificial Intelligence in Use Today*, FORBES (Jan. 10, 2017, 8:32 AM), https://www.forbes.com/sites/robertadams/2017/01/10/10-powerful-examples-of-artificial-intelligence-in-use-today.

4. *See* Ralph Jacobson, *2.5 Quintillion Bytes of Data Created Every Day. How Does CPG & Retail Manage It?*, IBM (Apr. 24, 2013), https://www.ibm.com/blogs/insights-on-business/consumer-products/2-5-quintillion-bytes-of-data-created-every-day-how-does-cpg-retail-manage-it.

5. The data security principles I adhere to are based on best practices promulgated by the National Institute of Science and Technology (NIST). *See* NAT'L INST. OF SCI. & TECH., SPECIAL PUBLICATION 800-53 REVISION 4: SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS 1 n.4 (2013), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf ("Security requirements are derived from mission/business needs, laws, Executive Orders, directives, regulations, policies, instructions, standards, guidance, and/or procedures to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted . . . ."). Even though NIST's primary mission is to provide security controls for federal information systems, the teachings in SP 800-53 are widely regarded as applicable to other industries. The Federal Trade Commission has elevated it to a quasi-legal standard, identifying it as the basis for legally reasonable data security practices. Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, FEDERAL TRADE COMMISSION: BUSINESS BLOG (Aug. 31, 2016, 2:34 PM), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc ("From the perspective of the staff of the Federal Trade Commission, NIST's Cybersecurity Framework is consistent with the process-based approach that

IoT-generated data—becomes the primary challenge facing IoT manufacturers, regulators, law makers, and consumers.

Notwithstanding industry observers' flavor for the dramatic, alarmist attitudes, none of the IoT cybersecurity threats are properly classified as "new." Every single one of these threats: hacking, exfiltration, malware, DDoS, and ransomware predates the emergence of IoT. Viewing the threat as evolving, rather than new, helps make it clear that contemporary best practices are still relevant for countering the IoT threat surface. Be they from the National Institute of Science and Technology (NIST), the Control Objectives for Information and related Technologies (COBIT), the International Standards Organization (ISO), the International Society of Automation (ISA), or the Federal Trade Commission (FTC), the best practices already exist. The ability to rely on proven methodologies in an operational environment where rampant, dynamic change (technological advancement and threat sophistication) is the only constant serves as a stabilizing force. In turn, these best practices can be used as a roadmap to help secure IoT device design and use.[6]

---

the FTC has followed since the late 1990s, the 60+ law enforcement actions the FTC has brought to date, and the agency's educational messages to companies, including its recent Start with Security guidance."). As such, it is reasonable to reference these cybersecurity best practices as having legal significance. In turn, this means that a device manufactured where they are absent is a device that is properly understood as not compliant with legally reasonable cybersecurity practices.

6. These threats get more sophisticated, and some will, at least initially in their lifecycle, be difficult to detect and defeat. *See, e.g.*, Andy Greenberg, *A Deep Flaw in Your Car Lets Hackers Shut Down Safety Features*, WIRED (Aug. 16, 2017, 4:55 PM), https://www.wired.com/story/car-hack-shut-down-safety-features/.

So, while the cyber threats to IoT themselves are not new, there are two markedly different attributes: (a) the threat surface itself, i.e., billions of devices and the quality of the data they generate are susceptible to compromise, and (b) the increasing sophistication and power of available computing platforms.[7] In case of the latter, the emergence of cyber weapons with Stuxnet-caliber capabilities,[8] quantum computing-powered

7. Google revealed that on its artificial intelligence (AI) applications "that utilize neural network inference, [its self-developed Tensor Processing Unit] TPU is 15 times to 30 times faster than contemporary GPUs and CPUs" such as NVidia and Intel. Stephanie Condon, *TPU Is 15x to 30x Faster than GPUs and CPUs, Google Says*, ZDNET (Apr. 5, 2017, 7:11 PM GMT), http://www.zdnet.com/article/tpu-is-15x-to-30x-faster-than-gpus-and-cpus-google-says/. This is significant because it dramatically impacts and accelerates the proliferation and power of deep learning AI algorithms. A corollary effect is the enhanced potential for expanding the availability of CLAI, as it is reasonably certain that NVidia and Intel will work hard to keep abreast, if not overtake, Google's TPU specs. Quantum computing is another emerging computing platform, though it is widely regarded as a paradigm changer, not merely an incremental step. *See* Tae Kim, *Morgan Stanley: This Next Big Technology Trend Could Start the 'Fourth Industrial Revolution'*, CNBC (Aug. 24, 2017, 1:43 PM EST), https://www.cnbc.com/2017/08/24/morgan-stanley-this-next-big-technology-trend-could-start-the-fourth-industrial-revolution.html. Open sourcing quantum computing offers a way to broaden and speed the development of quantum applications and quantum computing capabilities in general. One example of this is the D-Wave open source Qbsolv. *See* Klint Finley, *Quantum Computing Is Real and D-Wave Just Open-Sourced It*, WIRED (Jan. 11, 2017, 1:00 PM), https://www.wired.com/2017/01/d-wave-turns-open-source-democratize-quantum-computing/. Qbsolv is capable of solving large quadratic unconstrained binary optimization (QUBO) problems. As such, Qbsolv could be well-suited for building CLAI (e.g., in relation to QUBO application to pattern analysis). *See* Øivind Due Trier & Torfinn Taxt, *Evaluation of Binarization Methods for Document Images*, 17 IEEE TRANSACTIONS ON PATTERN ANALYSIS & MACHINE INTELLIGENCE 312–15 (1995). For data mining apps, see Haibo Wang, Bahram Alidaee & Gary A. Kochenberger, *Evaluating a Clique Partitioning Problem Model for Clustering High-Dimensional Data Mining*, AMCIS PROCEEDINGS (2004), https://www.semanticscholar.org/paper/Evaluating-a-Clique-Partitioning-Problem-Model-for-Wang-Alidaee/e84f4ebee1182e9c7874d2093791ce65dbef48db.

8. *See* Jeremy Richmond, *Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?*, 35 FORDHAM INT'L L.J. 842 (2012).

attacks,[9] ransomware with more robust encryption,[10] blockchain attacks,[11] lightweight block cipher compromise[12], etc., become candidates for representing the "new normal" threat basis. Combined, these variables considerably amplify the risks of using IoT devices, that is, they fuel an increased probability of

---

9. Quantum computers are millions of times more powerful than the most powerful computers we have today. Calculations that are practically impossible for even the most powerful contemporary computers (since the length of time they would require is measured in thousands of years) can take quantum computers mere seconds to resolve. *See What Is Quantum Computing?*, IBM, http://www.research.ibm.com/ibm-q/learn/what-is-quantum-computing/ (last visited Dec. 29, 2017). We're already in the midst of this change. In April 2014, IBM announced they succeeded in accomplishing a critical milestone with a 4-qubit chip. About a year later, Google more than doubled that, with a 9-qubit chip. Both achievements were done with the requisite self-error detection threshold that makes for reliable qubits; in other words, these companies achieved not a theoretical, but a viable quantum computing state. *See* Julian Kelly et al., *State Preservation by Repetitive Error Detection in a Superconducting Quantum Circuit*, NATURE 66 (2015). Microsoft, Northrop Grumman, Lockheed, Alibaba and others are pouring massive resources getting into the quantum game. Researchers at the University of New South Wales even managed to substitute expensive materials like cesium and diamonds with silicone. MIT Technology Review reports that IBM recently released a 50-qubit quantum computer, and is making a 20-qubit version available through its cloud computing platform. Google is (likely only temporarily) behind, but steaming ahead with its quantum supremacy project. While a 20-qubit platform is more powerful than a 9-qubit one (Google released its 9-qubit two years earlier), it will be interesting to see what benefit CLAI will have running on the more powerful qubit platforms. One possible benefit could be in dealing with more complex data mining applications and augmenting (e.g., features/capabilities) in mixed reality (MR) applications.

10. NIST has warned that SHA-1 is obsolete. *See* Lily Chen, *NIST Comments on Cryptanalytic Attacks on SHA-1*, NIST (Apr. 26, 2006), https://csrc.nist.gov/News/2006/NIST-Comments-on-Cryptanalytic-Attacks-on-SHA-1. Bruce Schneier, Chief Technology Officer at IBM Resilient and a fellow at Harvard University Berkman Center, shares an intriguing analysis of the costs of a practical collision attack on SHA-1 encryption, currently placing it at $173,000, and predicting $43,000 by 2021. *See* Bruce Schneier, *When Will We See Collisions for SHA-1?*, SCHNEIER ON SECURITY (Oct. 5, 2012, 1:24 PM), https://www.schneier.com/blog/archives/2012/10/when_will_we_se.html.

11. *See* Roger A. Grimes, *Hacking Bitcoin and Blockchain*, CSO (Dec. 12, 2017, 3:45 AM PST), https://www.csoonline.com/article/3241121/cyber-attacks-espionage/hacking-bitcoin-and-blockchain.html.

12. "Lightweight block cipher" refers to cryptographic methodologies used in applications that require low cost, energy efficient and small footprint characteristics. Lightweight block cyphers are used in RFID tags, field-programmable gate arrays, mobile devices, and smartcards. *See* ALEX BIRYUKOV, ARNAB ROY, & VESSELIN VELICHKOV, *Differential Analysis of Block Ciphers SIMON and SPECK*, 8540 LECTURE NOTES IN COMPUTER SCIENCE (2014), https://eprint.iacr.org/2014/922.pdf.

hacking highly valuable information and considerably complicate the effective execution of cybersecurity best practices.

Despite the abundant (and in many cases free)[13] availability of cybersecurity best practices, the persistent failure to manage their effective execution[14] challenges the realization of meaningful risk mitigation.[15] One of the most significant root causes for a cybersecurity breach is user error.[16]

From this, it becomes clear that augmented automation is necessary and artificial-intelligence-powered computational law applications (CLAI) are an essential part of this answer; they can make it possible to mitigate cybersecurity threats not just at the user level by generating more educated users but also at the device manufacturer level.[17] The bottom line benefit of having educated users is that it helps drive out companies that produce IoT devices that do not meet desired security thresholds.[18]

In this article, I begin by describing the IoT cybersecurity threat landscape and the tension it creates on effectively maintaining not only privacy, but also confidentiality, integrity

---

13. *See, e.g.*, NAT'L INST. OF SCI. & TECH., *supra* note 5, at 2; Arias, *supra* note 5.

14. *See* Richard Starnes, *Cybersecurity Recruitment in Crisis*, CSO (May 25, 2016, 10:33 AM PST), https://www.csoonline.com/article/3075293/leadership-management/cybersecurity-recruitment-in-crisis.html.

15. Anthony Grieco, *Why Poor Cyber Hygiene Invites Risk*, DARKREADING (Oct. 20, 2016), https://www.darkreading.com/attacks-breaches/why-poor-cyber-hygiene-invites-risk/a/d-id/1327235.

16. PONEMON INST., 2017 COST OF DATA BREACH STUDY 14 (June 2017), https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf.

17. STEVEN MAZUR ET AL., MITIGATING CLOUD COMPUTING SECURITY RISKS USING A SELF-MONITORING DEFENSIVE SCHEME 4 (2011); *see* Nicole Meyers, *Artificial Intelligence Offers New Ways to Improve Consumers' Financial Health*, THE FINANCIAL BRAND (June 27, 2017), https://thefinancialbrand.com/66065/artificial-intelligence-financial-wellness-literacy-banking/ (succinctly describing AI's applications in educating users in the financial sector, a principle transferrable to this article).

18. Majid Ahmed, *Why Smart Consumers Are Key to IoT Security*, NETWORKWORLD (Oct. 13, 2017, 6:16AM PST), https://web.archive.org/web/20180130104657/https://www.networkworld.com/article/3231999/internet-of-things/why-smart-consumers-are-key-to-iot-security.html; *see* Ben Rossi, *Educating the End User and Eliminating the Biggest Security Risk*, INFORMATION AGE (June 19, 2014), http://www.information-age.com/educating-end-user-and-eliminating-biggest-security-risk-123458150/ (the proposition of this article—that educated users make better, more secure choices in an active software use environment, and thus, reduce enterprise risk—translates to the hardware and software requisitioning environment as well by the same logic).

and availability of the collected data. The second part introduces and defines the relationship between artificial intelligence (AI) and computational law, which serves as a segue to the third section which reviews how the product of the combination of the two, the CLAI, can help mitigate the cybersecurity threat. The fourth part describes the "information broker" function played by the CLAI, laying out the data points that the CLAI can evaluate for the delivery of actionable information to the end-user.

II. THE IOT THREAT SURFACE

With billions of devices connected to countless aspects of our daily lives, systematically recording our sleep patterns, food intake, weight, heart rate, exercise patterns, blood sugar levels, temperature preferences, electricity use, driving speed, location, etc., then transmitting all of this data to the cloud, what could possibly go wrong? Pretty much everything.[19] Thus, the IoT threat surface should be viewed with significant deference, using a prism that encourages the use of effective risk mitigation techniques. By referencing/evaluating it through what I call the "AI Risk Ratio" it is possible to design effective tools (applications and policies) to manage risk to optimal levels. Through the AI Risk Ratio, we see that the greater the computing power of AI that is integrated or used with a given IoT device, the greater the probability that the specific device will be capable of generating, storing, and transmitting higher-quality data.[20] Hacking risks are properly considered as elevated

---

19. NAT'L INST. OF SCI. & TECH., SPECIAL PUBLICATION 800-160: SYSTEMS SECURITY ENGINEERING ii (2016), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf ("With the continuing frequency, intensity, and adverse consequences of cyber-attacks, disruptions, hazards, and other threats to federal, state, and local governments, the military, businesses, and the critical infrastructure, the need for trustworthy secure systems has never been more important to the long-term economic and national security interests of the United States. Engineering-based solutions are essential to managing the growing complexity, dynamicity, and interconnectedness of today's systems, as exemplified by cyber-physical systems and systems-of-systems, including the Internet of Things.").

20. As used in this paper, "data quality" is a function of the resources required to generate it plus the likelihood of harm it can cause if used for ill gain. As such, data quality is driven by the type and sophistication of the device used. A NEST thermostat, for example, generates, stores and transmits HVAC use data that has lower quality than that generated, stored and transmitted by an implantable medical device.

in those devices that garner a high AI Risk Ratio score, which means that more robust protections need to be brought into play.

Let's start with a quick visit to the issue of privacy. Depending on your views on the matter, Scott McNealy's observation that we have "zero privacy anyway" and that we should "get over it"[21] is either accurate and a call to cease obsessing over it or a highly inadequate stance. For those who applaud McNealy's view, its seductive attribute of a quick and simple remedy to vexing privacy questions is satisfying. For those who decry it, it is an attitude that is in equal parts myopic, impractical, psychologically unsatisfying, economically unsound, and altogether unnecessary.

We intuitively recognize that privacy is an important principle. Through the plethora of laws, regulations, rules, policies, and standards that are designed to protect it, we can witness the significant resources that have poured into the effort to ensure that the use of private information is carefully regulated. Private information is, after all, our metadata, delivering information about our behavior, wants, and needs, all of which are the ingredients for developing efficient marketing campaigns, new product and service offerings, and deploying other tactics for increasing a company's sales and market share. Of course, these very same attractive attributes also lure nefarious players: the hackers, internet-era pirates insatiably thirsting for private information to fuel credit card fraud, theft, ransomware, and other illegal ventures.

Despite the near impossibility of a precise identification of the monetary value of private information, a fact encountered by many post-data breach plaintiffs,[22] the task of securing[23] that information remains legally obligatory. This information security task should also be regarded as a paramount ideal, a design principle, for IoT device manufacturers and their supply

---

21. *See* Polly Sprenger, *Sun on Privacy: 'Get Over It'*, WIRED (Jan. 26, 1999, 12:00 PM), https://www.wired.com/1999/01/sun-on-privacy-get-over-it/.

22. *See, e.g.*, *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 30 (D.D.C. 2014); *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 660 (S.D. Ohio 2014).

23. Security is defined as "freedom from those conditions that can cause a loss of assets with unacceptable consequences." NAT'L INST. OF SCI. & TECH., *supra* note 19. The authors of S.P. 800-160 note that the definition of security "is adapted from similar concepts defined by the National Aeronautics and Space Administration (NASA) for safety and system safety." *Id.* at 13 n.15.

chain. Essentially, executing this principle incorporates the privacy and security by design paradigms.

Successfully contending with the threats to confidentiality (of which privacy is a subset), integrity of availability in an IoT ecosystem that contains billions of devices, trillions in market value, and zettabytes of valuable data, is daunting.

III. ARTIFICIAL INTELLIGENCE AND COMPUTATIONAL LAW

Drama and fantasy renditions have served to corner artificial intelligence (AI) into a dystopian milieu dominated by scheming computers and killer robots that have taken over the world and decimated humanity. The reality of AI is, of course, relatively much more mundane. AI is really just the "the study of cognitive processes using the conceptual frameworks and tools of computer science."[24] Taking this a step further and keeping in mind the practical purposes of this paper, it is sufficient to understand AI in the context of what is known as "machine learning"[25] and in the role of an automated virtual assistant.[26]

The behavioral term "learning" is descriptive of the process by which a computer program modifies its performance in direct reaction to a particular set of parameters existing in its operating environment at any given point in time.[27] Each

---

24. *See* Edwina L. Rissland, *Artificial Intelligence and Law: Stepping Stones to a Model of Legal Reasoning*, 99 YALE L.J. 1957 (1990).

25. *See* Nils J. Nilsson, Introduction to Machine Learning (Nov. 3, 1998) (unpublished manuscript) (available at https://ai.stanford.edu/~nilsson /MLBOOK.pdf); L. Thorne McCarty, *How to Ground a Language for Legal Discourse in a Prototypical Perceptual Semantics*, 2016 MICH. ST. L. REV. 511 (2015).

26. Some of the popular consumer versions are currently embodied in Siri, Alexa, Cortana and Google Assistant.

27. Nilsson, *supra* note 25, at 1–3. In the context of computational law, terms and conditions in a contract comprise a set of parameters that affect and influence the AI's learning. These parameters are also not always static, as companies frequently state that they reserve the right to modify them at any time after the purchase. *See* Mark Lemley, *Terms of Use,* 91 MINN. L. REV. 459, 475 n.55 (2006). *See generally* Logan Koepke, *"We Can Change These Terms at Anytime": The Detritus of Terms of Service Agreements*, MEDIUM (Jan. 18, 2015), https://medium.com/@jlkoepke/we-can-change-these-terms-at-anytime-the-detritus-of-terms-of-service-agreements-712409e2d0f1. An AI usable in computational contract law should be able to continuously evaluate and score whether or not a given provision qualifies as a misrepresentative statement or whether it is sufficiently innocuous (within the traditional economic theory of cost-benefit analysis). *See* Richard Craswell, *Taking Information Seriously:*

learning instance, or modification, occurs for the purpose of enhancing the AI's performance in terms of speed and accuracy. Thus, the AI's capability to learn is a desirable attribute because it enables the application to successfully handle tasks that are not conducive to predetermined actions (by the coder).[28] This is an especially important capability when it comes to dealing with zettabyte-scale data.[29]

Computational law refers to a subset of study in legal informatics[30] that deals with coding the law, i.e., representing the law (in relevant part, contracts[31] and cybersecurity industry

---

Misrepresentation and Nondisclosure in Contract Law and Elsewhere, 92. VA. L. REV. 565, 606–07 (2006).

28. *See* Nilsson, *supra* note 25, at 2–3.

29. *Id.* at 3 ("The amount of knowledge available about certain tasks might be too large for explicit encoding by humans. Machines that learn this knowledge gradually might be able to capture more of it than humans would want to write down.").

30.

> The management of information is crucial to the proper functioning of any legal system. A good legal system relies on information about the world itself (such as evidence of who did what and when) as well as more purely legal information (such as court rulings, statutes, contracts, and so forth). Legal Informatics is the theory and practice of managing such information. It covers both legal theory and information theory. It also covers elements of general information processing technology as well as applications of that technology in the administration of law. While the concept of Legal Informatics is not new, its importance is greater than ever due to recent technological advances – including progress on mechanized legal information processing, the growth of the Internet, and the proliferation of autonomous systems (such as self-driving cars and robots), as well as globalization of the legal industry.

Legal Informatics, STANFORD LAW SCHOOL: COURSE CATALOG, https://law.stanford.edu/courses/legal-informatics/ (last visited Jan. 8, 2018).

31.

> But now we're almost ready, I think, for computational law. Where for example contracts become computational. They explicitly become algorithms that decide what's possible and what's not. You know, some pieces of this have already happened. Like with financial derivatives, like options and futures. In the past these used to just be natural language contracts. But then they got codified and parametrized. So they're really just algorithms, which of course one can do meta-computations on, which is what has launched a thousand hedge funds, and so on.

standards[32]) in computer code.[33] Coding simplifies the law, renders it more accessible and understandable to non-lawyers, and as such is deemed a desirable pursuit.[34]

Combining AI with computational law results in a relatively much more capable application. A CLAI is capable of quickly and accurately performing significantly more elaborate computational processes than its non-AI counterpart.[35] This, of course, is not intended to imply that all computational law applications must have an AI engine to qualify as a valid computational law application. It can be expected, however, that as the computing capabilities of AI grow, and the range and sophistication of desired capabilities/transactions increases, the rationale for excluding AI from a computational law application will be diluted.

IV. MITIGATING THE CYBERSECURITY THREAT WITH COMPUTATIONAL LAW ARTIFICIAL INTELLIGENCE APPLICATIONS

The cybersecurity threats to the confidentiality (and its privacy subset), integrity and availability of IoT-generated data can be more effectively dealt with so long as end-users become markedly more educated about the IoT devices they use. Attaining this status requires putting in place tools that enable end-users to make meaningful, optimal choices. These tools come in the form of CLAI.

At the device purchase stage, it means the CLAI helps drive the end-user's decision to purchase a certain IoT device, which means the CLAI is capable of presenting the end-user with an efficient amount of information that enables the end-user's substantive purchase analysis (i.e., diluting some of the

---

Stephen Wolfram, *Talking About the Computational Future at SXSW 2013*, STEPHEN WOLFRAM: BLOG (Mar. 19, 2013), http://blog.stephenwolfram.com/2013/03/talking-about-the-computational-future-at-sxsw-2013/.

32. *See, e.g.*, NAT'L INST. FOR STANDARDS AND TECH., *supra* note 6.

33. *See, e.g.*, M. J. Sergot et. al, *The British Nationality Act as a Logic Program*, 29 COMMUNICATIONS OF THE ACM 370, 370–85 (1986); Michael Genesereth, *Computational Law: The Cop in the Back Seat*, STANFORD U., complaw.stanford.edu (last visited Jan. 5, 2018).

34. *See* Genesereth, *supra* note 33 (noting that computational law "has the potential to bring legal tools to everyone in society . . . .").

35. *See* Gideon Lewis-Kraus, *The Great A.I. Awakening*, N.Y. TIMES MAGAZINE, Dec. 14, 2016, https://www.nytimes.com/2016/12/14/magazine/the-great-ai-awakening.html.

emotional-based decision points). During the post-purchase phase, the CLAI enables the end-user to remain systematically, continuously informed about the IoT device and take action when it becomes necessary throughout the useful life of the device. [36]

Substantive purchase and post-purchase decisions on IoT devices are difficult to make because of the anemic amount of accessible information. This constraint chokes off the end-user's ability to make an educated purchase and use decision, which magnifies the cybersecurity risks associated with using that particular device.

Consider, for example, that each IoT device is bundled with a warranty and other legally binding and/or legally significant attributes that an end-user needs to be able to effectively deal with in order to qualify as an educated end-user.[37] Of course, the main challenge in getting to the point where an end-user is properly deemed "educated" is the absence of the necessary tools. Without these tools, end-users surrender to the "impenetrability"[38] of the legalese that is wrapped around these tools and this reduces the effectiveness of the end-user's ability to interact with the IoT device. For the purposes of this paper, this is a critical defect because there is a direct correlation between an end-user's knowledge of the IoT device, or lack thereof, and increasing the probability of perpetuating a cybersecurity risk.

The result is that in today's contracting environment (not just in the IoT realm), consent to the various legalese is provided by an end-user as an exercise of mere formality that, while

---

36. *See, e.g.*, Press Release, Electronic Toy Maker VTech Settles FTC Allegations That It Violated Children's Privacy Law and the FTC Act, Fed. Trade Comm'n (Jan. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated.

37. This is particularly important considering the fact that many manufacturers reserve the right to modify their legal terms at any time and without prior notice.

38. Amitai Etzioni, *The Privacy Merchants: What Is to Be Done?* 14 U. PA. J. CONST. L. 929, 942 (2012) ("[T]hat the fact that few consumers read [terms and conditions] shows they do not care; in actuality, data already cited strongly suggest that they do not read them because they find them impenetrable." (citing *FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses and Policymakers*, FEDERAL TRADE COMMISSION (Dec. 1, 2010), https://www.ftc.gov/news-events/press-releases/2010/12/ftc-staff-issues-privacy-report-offers-framework-consumers)).

arguably legally valid, is devoid of any other meaning.[39] The end-user has no idea as to what she agreed to, or what rights she might have had that were relinquished in a blink of an eye. The entire transaction was culminated based on nothing but flashy marketing materials. This transactional environment compromises cybersecurity and should be normatively unacceptable as the cybersecurity stakes in the IoT ecosystem are too high for such an informal attitude.

V. CLAI AS INTELLIGENT INFORMATION BROKERS

CLAI can help ameliorate the cybersecurity risk. The CLAI can be incorporated into or work alongside (as a separate application) IoT devices in the drive toward implementing and augmenting privacy and security by design features, which promote the confidentiality/privacy, integrity and availability of the information collected. This is achieved by the CLAI acting as an information broker, providing the end-user with actionable advice about the IoT device in a timely manner. The "actionable" attribute is important as it denotes the optimized nature of the information provided, meaning that it is presented to the end-user in a way that is designed to maximize the opportunity for an informed decision to be reached in a timely manner.[40]

Thus the CLAI is a tool by which to attain the goal of promoting an IoT cybersecurity ecosystem that is dominated by educated IoT end-users, an ecosystem in which end-users are less likely to make mistakes that compromise the confidentiality/privacy, integrity and availability of the data collected by the their IoT devices.[41] And as end-users become better educated about the IoT devices they use, they can also more efficiently participate in the IoT ecosystem, ultimately selecting those devices that carry the most consumer-friendly

---

39. *See* Lemley, *supra* note 27, at 465–67.

40. Craswell, *supra* note 27, at 575.

41. Consumers, generally speaking, have a poor understanding of the technology they use. *See* Sharyn Jackson, *You've Got Someone Else's Mail: Digital Doppelgangers Find In-box Surprises*, STAR TRIB. (Aug. 25, 2017, 4:44 PM), http://www.startribune.com/do-you-have-a-digital-doppelganger-how-to-protect-yourself-from-errant-e-mails/441675103/. The problem with an uneducated user is that they are more susceptible to propagate local or even widespread cybersecurity problems.

warranty, terms and conditions[42] and meet or exceed cybersecurity best practices.

There are a number of possible CLAI implementations. For instance, a CLAI can be used to distill and compare relevant IoT device information from multiple sources and deliver a succinct message (referred to as a "signal") to the end-user. Of course, an end-user could also select to be advised through other means, such as a chat session. Some CLAI applications can also feature distinct default (though still user-configurable) communication formats that depend on the IoT device they are tasked with providing information on. For example, the communication protocol for a smart home lighting kit can be easily accommodated by signaling (icons, emoji), as the more complex chat format is likely unnecessary (but still available should the end-user desire it).

Toggling between simple action signals and the more complex chat interface can be driven by the CLAI's assessment of multiple reference points that comprise the particular IoT device. An illustrative list includes: (a) existence of unfavorable terms and conditions (a poor warranty[43]); (b) litigation frequency (manufacturer has a-greater-than certain amount of relevant litigation in any given year[44] and/or has been the subject of enforcement actions by the FTC[45]); (c) evaluation of conformance with privacy and security-by-design principles; (d) identification of compliance, or lack thereof with cybersecurity best practices[46]

---

42. "Terms of use are no less a part of 'the product' than are the size of the database and the speed with which the software compiles listings." ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1453 (7th Cir. 1996).

43. A "poor warranty" is the result from a comparison of every known warranty in a central repository. This is the subject of research at CodeX. At a high level, warranty information is constructed from data mining bots. *See also*, *HTC America Inc., In the Matter of*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter (last updated July 2, 2013) (connecting the automated assistant to an active ontology).

44. Lex Machina delivers this information today. Lex Machina was a project born from Stanford Law School's Center for Computational Law (CodeX). Lex Machina was sold to Lexis.

45. FED. TRADE COMM'N, *supra* note 36.

46. *See supra* note 5 and relevant discussion on the legal significance of cybersecurity best practices. CLAI also promotes the "Core" cybersecurity best practices, which are "five concurrent and continuous functions—Identify, Protect, Detect, Respond and Recover." Arias, *supra* note 5. The Core is a strategic view of the lifecycle of an organization's management of cybersecurity risk. Consider, for example, that in *HTC America Inc., In the Matter*

and with FTC consent decrees; (e) manufacturer-issued security and privacy notices;[47] and (f) user's risk tolerance profile.[48] When any of these monitored parameters meet or exceed a certain set threshold, the CLAI generates its score and alerts the user with an actionable symbol, such as a red flag.

Imagine asking your CLAI assistant whether it recommends that you purchase a certain ACME heart rate monitor. The CLAI's response advises that ACME ranks poorly because it contains misrepresentational attributes that render its warranty subpar,[49] its website's terms and conditions fall short of providing reasonable data security assurances (regarding uploaded data and its transmittal), and it is currently embroiled in class action litigation over poor battery life.[50]

---

of, FEDERAL TRADE COMMISSION, https://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter (last updated July 2, 2013) and *TRENDnet, Inc., In the Matter of*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter (last updated Feb. 7, 2014), the companies were accused of neglecting to implement basic security monitoring processes, specifically receiving, addressing, or monitoring vulnerabilities. CLAIs can automate the threat and vulnerability monitoring process.

47. FED. TRADE COMM'N, *supra* note 36.

48. The profile is rendered through a series of questions presented to the user. As the CLAI learns more about the user's behavior, such as her interaction with other IoT devices, the risk tolerance profile is updated, which can impact future signaling events, such as increasing or decreasing their frequency. *See also*, SPY Car Act of 2015, S. 1806, 114th Cong. (2015), https://www.blumenthal.senate.gov/imo/media/doc/SPY%20Car%20legislation%20BlumenthalMarkey%2020150721.pdf (last visited Jan. 15, 2018). It seeks (among other things) to protect drivers from security and privacy risks through the development of a "cyber dashboard" rating system. The dashboard concept is representative of the actionable information principle, providing consumers with an efficient representation of information, in this case how well the vehicle protects the driver from cyber-related risks.

49. Which attributes are symptomatic of a sub-par warranty can be built from case law and deposited into an ontology, which a CLAI can reference. Professor Craswell offers *Johnson v. Hewlett Packard Co.,* No. CX-01-1641, 2002 WL 1050426, at *1 (Minn. Ct. App. May 22, 2002) to illustrate how (potentially) intentional use of vague terms can influence a purchase decision. Though *Johnson* did not involve an IoT device, HP's use of inexact language in its printer advertising raised triable issues as to whether the language was sufficiently clear. By referencing an ontology of cases such as *Johnson* the CLAI can make a determination of whether the express warranties (advertising materials) match persistent identifiers of warranties associated with devices that should not be purchased.

50. This interaction can also be delivered through a CLAI chat session, though caution is required so as not to become tangled in complex unauthorized practice of law issues. The AI conversational platform offered by Chirrp offers

Conversely, if you purchase a device that received a "good" score from your CLAI, that CLAI will also keep you up to date whenever one more material events occur, such as the initiation of litigation against the manufacturer, etc. The CLAI will also be on the lookout for alternatives to the purchased IoT device should it conclude that continued use does not match your risk tolerance profile.[51]

Typically, the most likely recourse for an unsatisfied end-user is to switch off the device and/or return it. However, a CLAI could offer additional remedial options.[52] What they consist of depends on the type of device, the type of failure and the end-user's preferences, including their risk tolerance profile.

Medical device deviation from the established risk tolerance profile can lead the CLAI to alert the end-user to the nature of the deviation and offer a legal solution. For example, an action by the device that violates the privacy policy is a failure that may be remedied through an automated dispute settlement (which may include reporting to the FTC).[53] A more severe failure may trigger a recommendation to return the IoT device and replace it with another. In contrast, an operational deviation by a smart refrigerator could trigger a warranty claim filing by the CLAI. The range of legal remedies does not need to stop there and could include the filing of a complaint and the administration of an appropriate remedy. Of course, the legal infrastructure will need to be built to support those types of legal transactions, ensuring that there is an appropriate remedy-enforcement mechanism in

---

a useful illustration for how the interaction would be accomplished. *See* Nancy Dahlberg, *Chatting with Chirrp: Miami Company Uses AI to Engage with Customers*, MIAMI HERALD (Jan. 14, 2018, 9:00 AM), http://www.miamiherald.com/news/business/biz-monday/article194332219.html.

51. Ensuring the user is consistently appraised of important events, i.e., those that could affect the user's legal rights, the CLAI operates throughout the device's lifecycle. Some of the information from which to build these alternatives can be referenced from crowd-sourced recommendations and site search engines (e.g., Amazon's users-who-bought-this recommendations). As the AI engines become more sophisticated and CLAI networks become more robust, other CLAI-based recommendation sources could be leveraged.

52. Automated dispute mechanisms managed by CLAIs can help reduce litigation costs and relieve courts from being inundated with lawsuits.

53. *See e.g.*, Samuel Gibbs, *Chatbot Lawyer Overturns 160,000 Parking Tickets in London and New York*, GUARDIAN (June 28, 2016), https://www.theguardian.com/technology/2016/jun/28/chatbot-ai-lawyer-donotpay-parking-tickets-london-new-york.

place. IoT manufacturers could also use a CLAI to manage CLAI-filed claims against their supply chain.

VI. CONCLUSION

Educated end-users are the game changer for helping make the IoT ecosystem safer from a cybersecurity perspective. This observation is also supported by careful reading of the voluminous cybersecurity best practices, be they from NIST, COBIT, ISO and the others mentioned at the outset of this article. Without fault, all of these resources reflect the axiom that end-users play a vital role helping effectively manage cybersecurity risks; after all, they are the number one cause of problems in the first place. The same reading of these best practice resources also reveals that end-users can only really effectively perform their role if they are sufficiently educated about the devices they use. This may have been a relatively simple task before the dawn of IoT, but as the operational environment becomes larger and more sophisticated, the cybersecurity challenges and risks are significantly magnified. And because of the large number of variables that attach to each IoT device, it is necessary to deploy smart tools such as the CLAI. This intelligent information broker enables end-users to attain sufficient, substantive knowledge about the IoT devices they use. Once we pivot into an environment where end-users are educated by CLAI, we stand a better chance of maintaining a reasonably secure IoT cybersecurity environment.

***